Privacy Skills Needed for the Future

Applying Privacy Patterns to the Internet of Things' (IoT) Architecture

Dr. Sebastian Pape

Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt

September 13th 2019 Transform Bern

Agenda

- Introduction
  - Fog / Edge Computing
  - Privacy Patterns
  - Smart Vehicles
- Applied Privacy Patterns
- Summary Conclusion

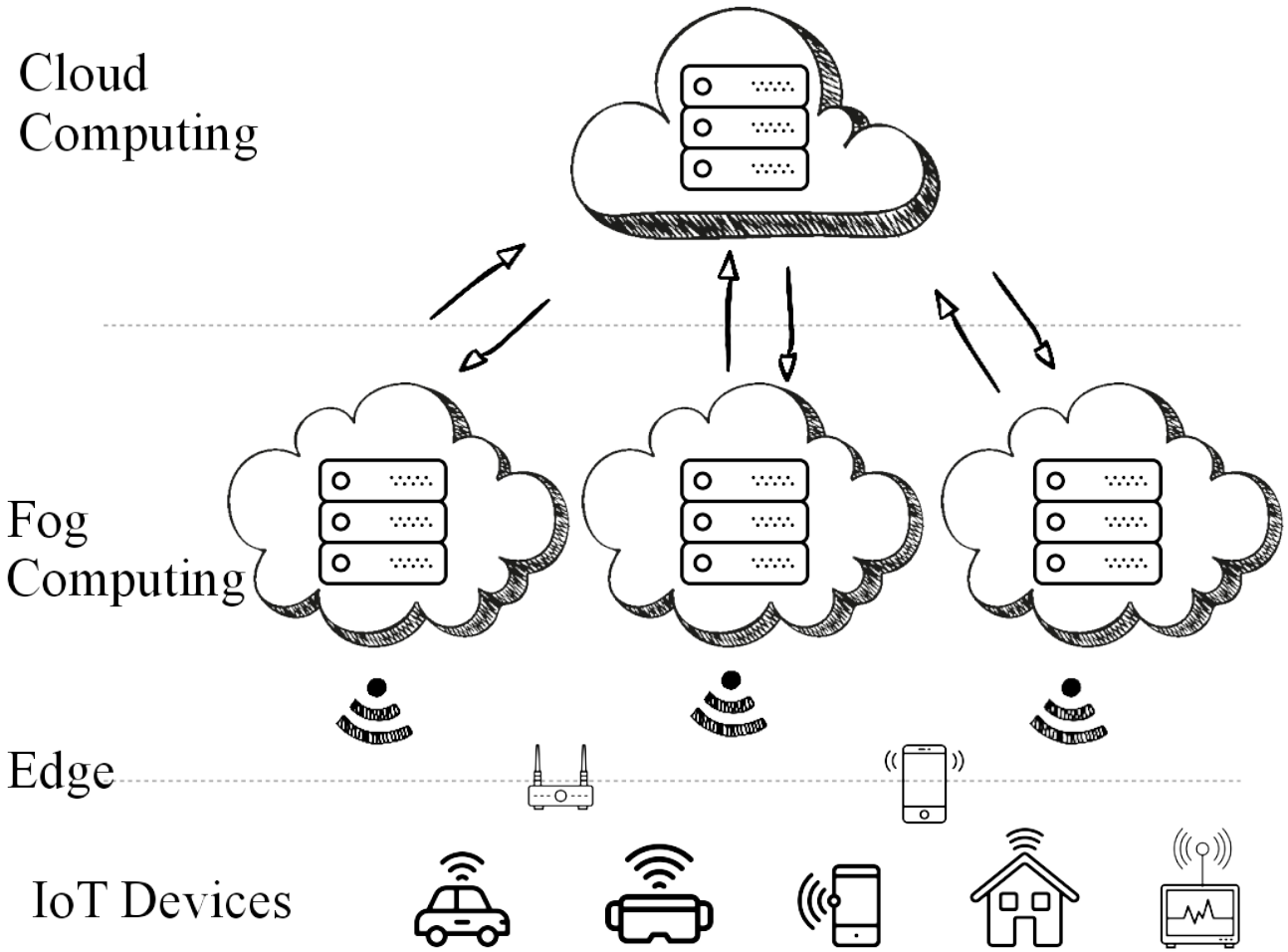
Introduction

- New Technologies / Architectures arise
  - Often because of certain requirements

- How can they be used to improve / sustain privacy?

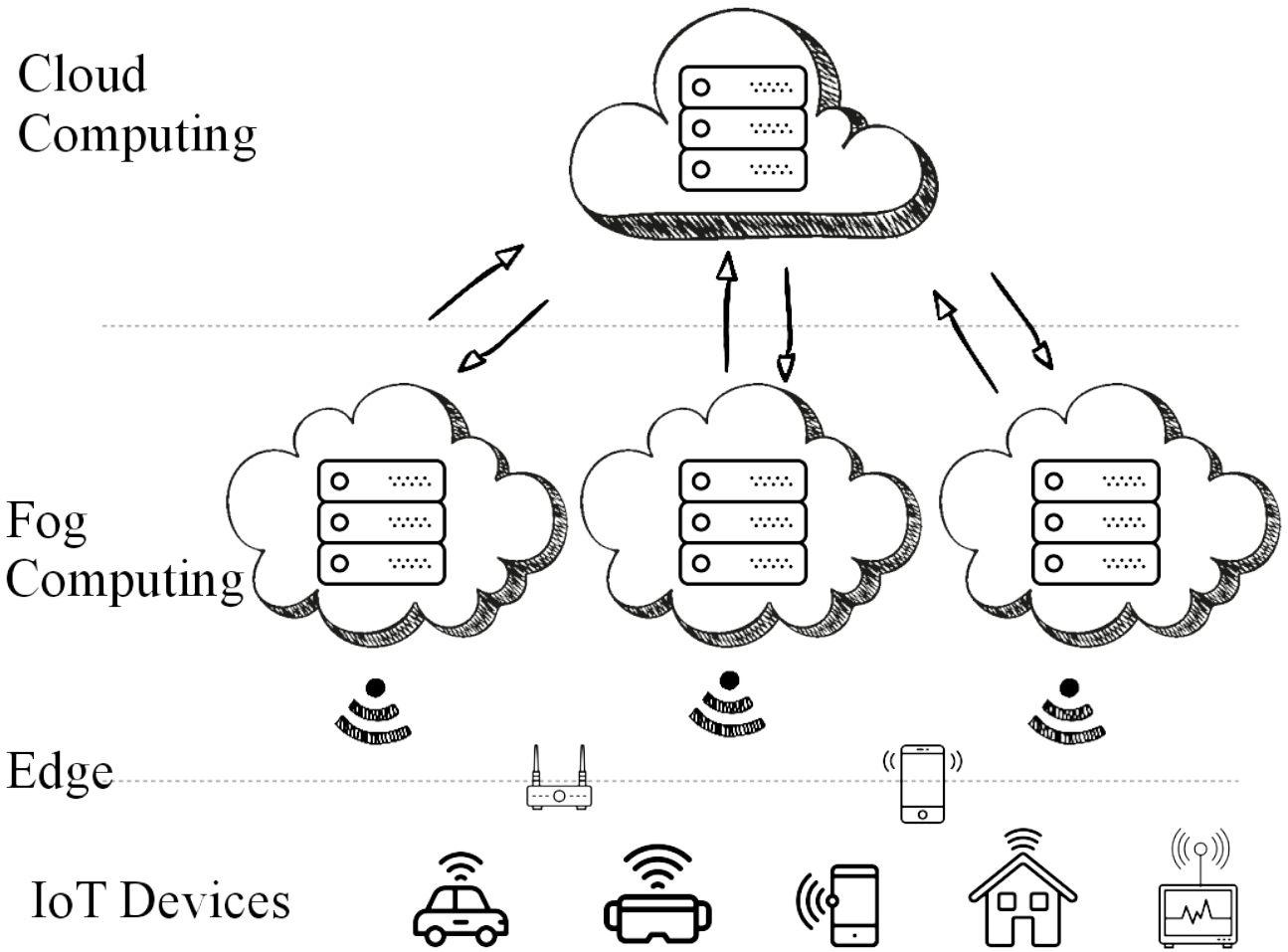
→ Example: Fog Computing

Fog Computing Conceptional Model (Three-layer Service Delivery Model)



[NIST Special Publication 500–325]

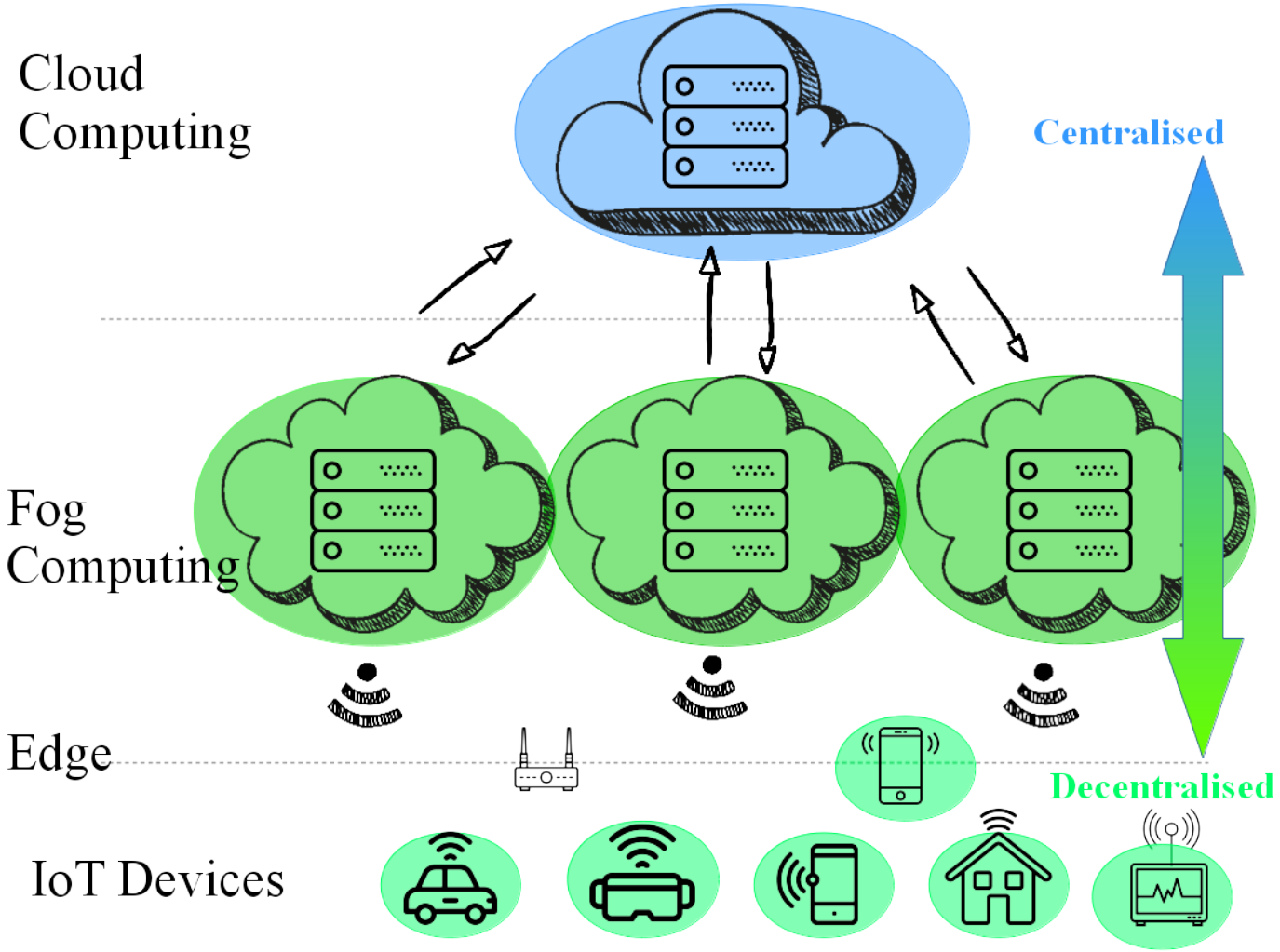
Fog Computing Conceptional Model (Properties)



- Low latency
  - Real-time interactions
- Geographical distribution
- Contextual location awareness
- Heterogeneity
- Interoperability
- Scalability and agility of federated, fog-node clusters
- Edge analytics

[NIST Special Publication 500–325]

Fog Computing Central / Decentral



Privacy Patterns

- Patterns describe
  - Already known solutions
  - Best practices

- Privacy patterns
  - Subset of design patterns
  - Translate privacy-by-design to practical advice

  → Privacy pattern libraries exist

CATEGORIES: CONTROL · SEPARATE · ISOLATE

Personal Data Store

Summary

Subjects keep control on their personal data that are stored on a personal device.

Context

The pattern is applicable to any data produced by the data subject (or originally under his control) as opposed to data about him produced by third parties.

Problem

Data subjects actually lose control over their data when they are stored on a server operated by a third party.

Solution

A solution consists in combining a central server and secure personal tokens. Personal tokens, which can take the form of USB keys, embed a database system, a local web server and a certificate for their authentication by the central server. Data subjects can decide on the status of their data and, depending on their level of sensitivity, choose to record them exclusively on their personal token or to have them replicated on the central server. Replication on the central server is useful to enhance sustainability and to allow designated third parties (e.g. health professionals) to get access to the data.

Enhance the control of the subjects on their personal data.

Consequences

Data subjects need to be equipped with a personal data store.

Contents

Privacy Relevant Information in IoT

- Identity Information:
  - e.g. name, address, telephone number, credit card number
- Data: Various sensitive information
  - e.g. user's preferences, occupation, health status and political inclination.
- Usage Information:
  - e.g. the readings of a smart meter
- Location Information:
  - Attacker is able to identify a user's trajectory, identity, points of interest

↯ Privacy vs. use of online services, i.e. navigation and LBS

[Ni J, Zhang K, Lin X, Shen X (2017) Securing fog computing for internet of things applications: Challenges and solutions. IEEE Communications Surveys & Tutorials]

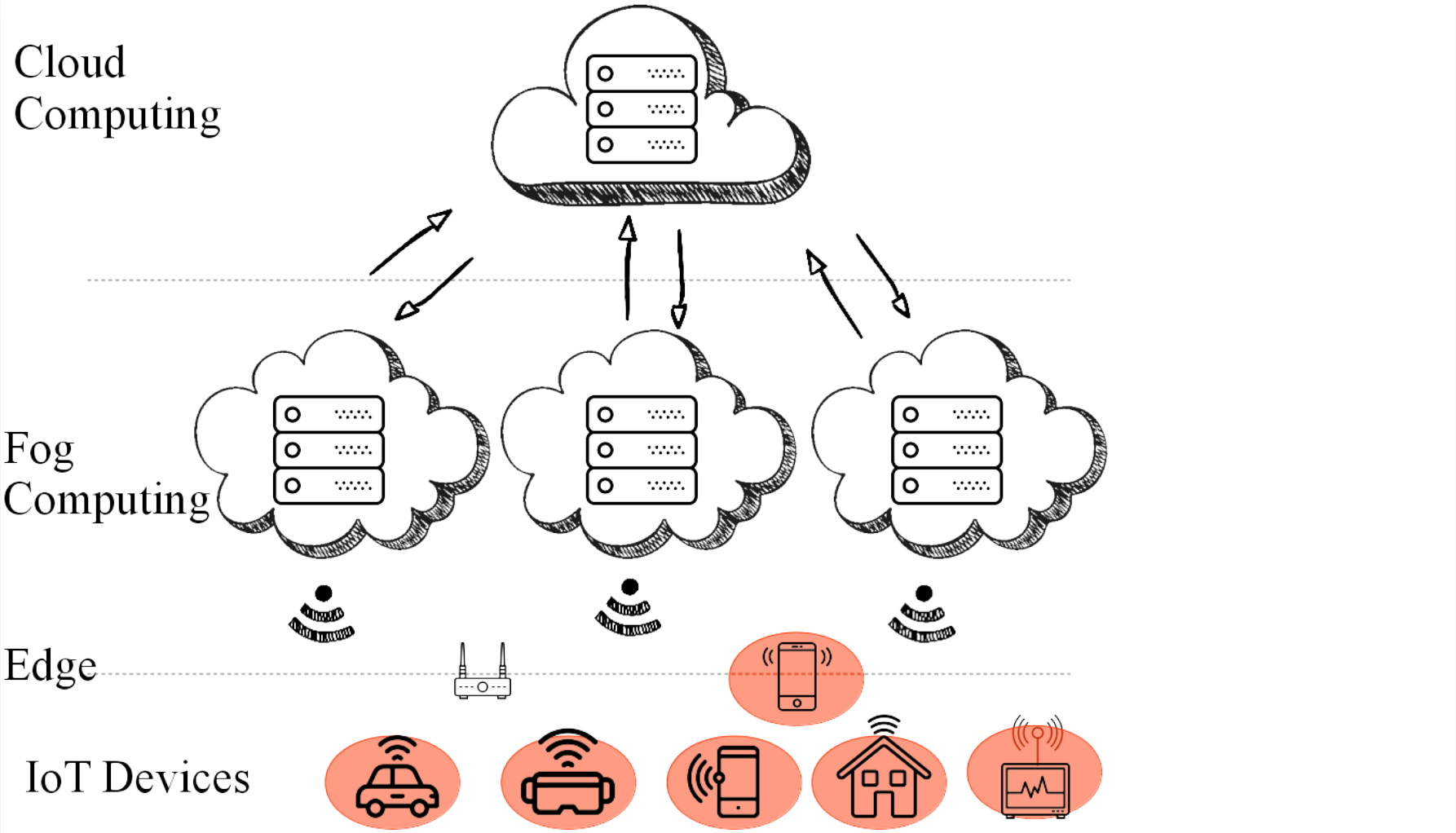
Smart Vehicles Scenario
Autonomous valet parking

- Driving robot
  - parks the vehicle at nearby or remote location
    - after users exited & cargo is unloaded
  - drives the vehicle from parking lot to a desired destination

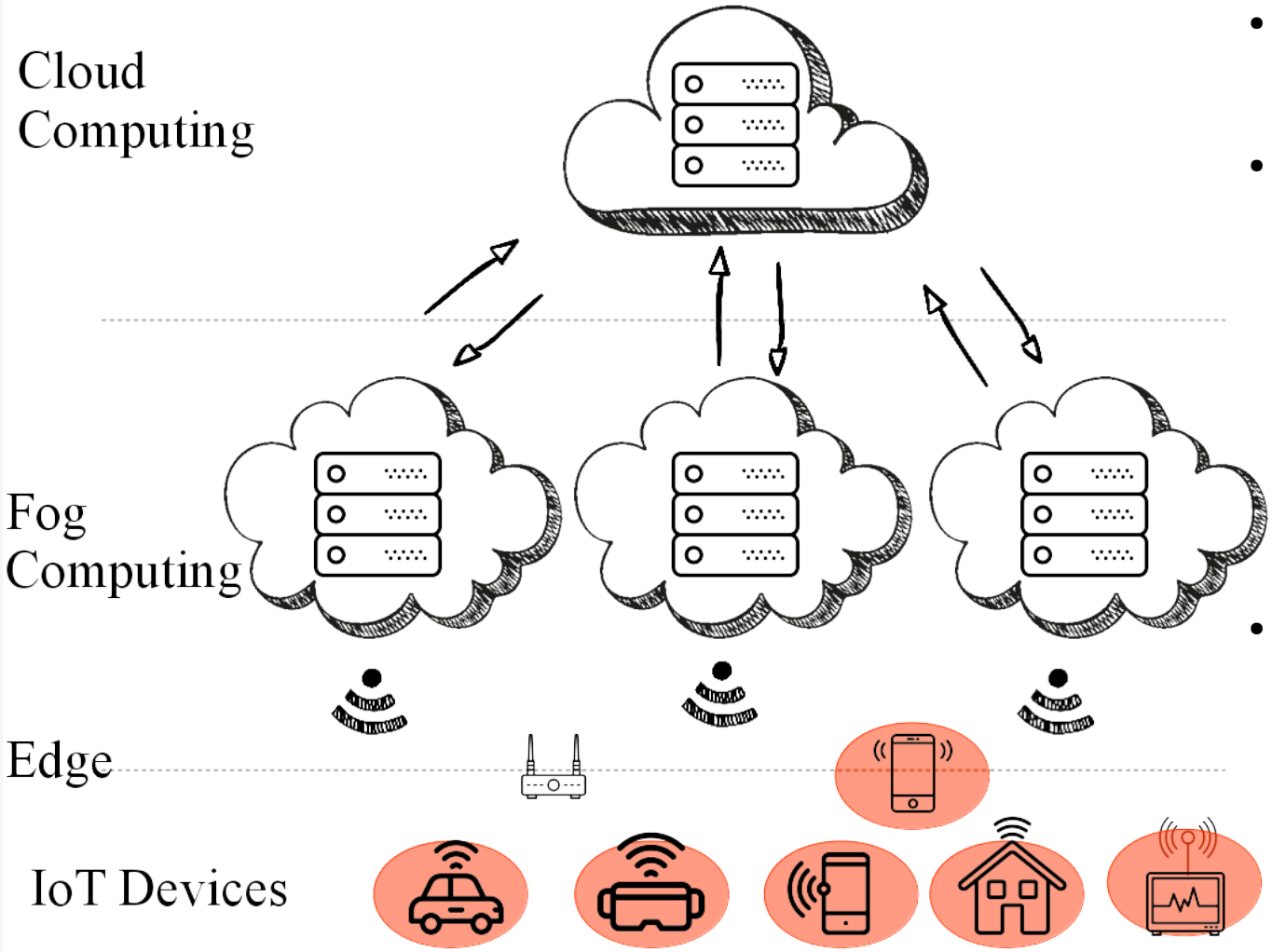
- Advantages
  - Driver saves time
  - Parking space used more efficiently

- Assumption
  - Fog node at each parking lot

Personal Data Store



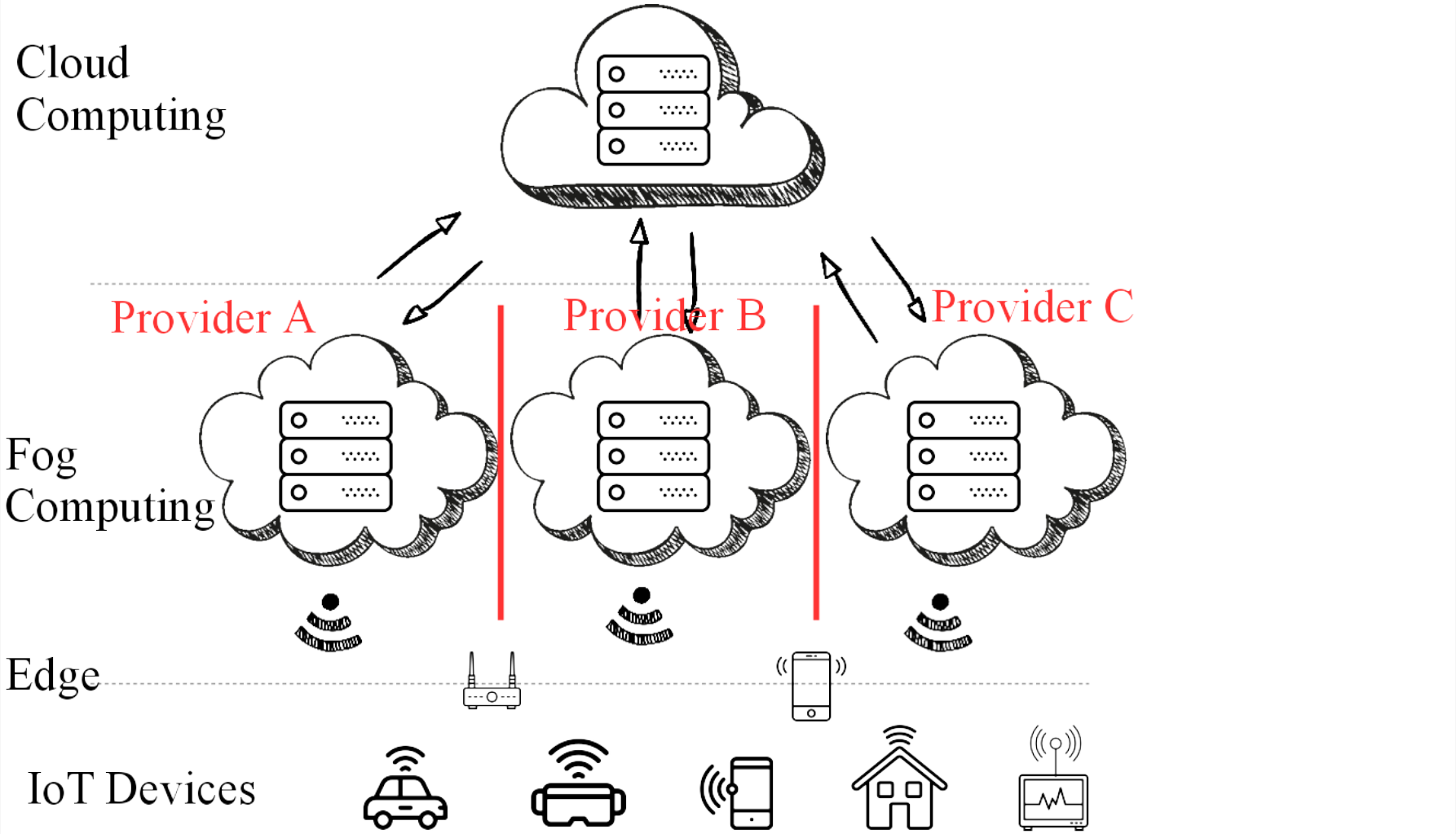
Personal Data Store



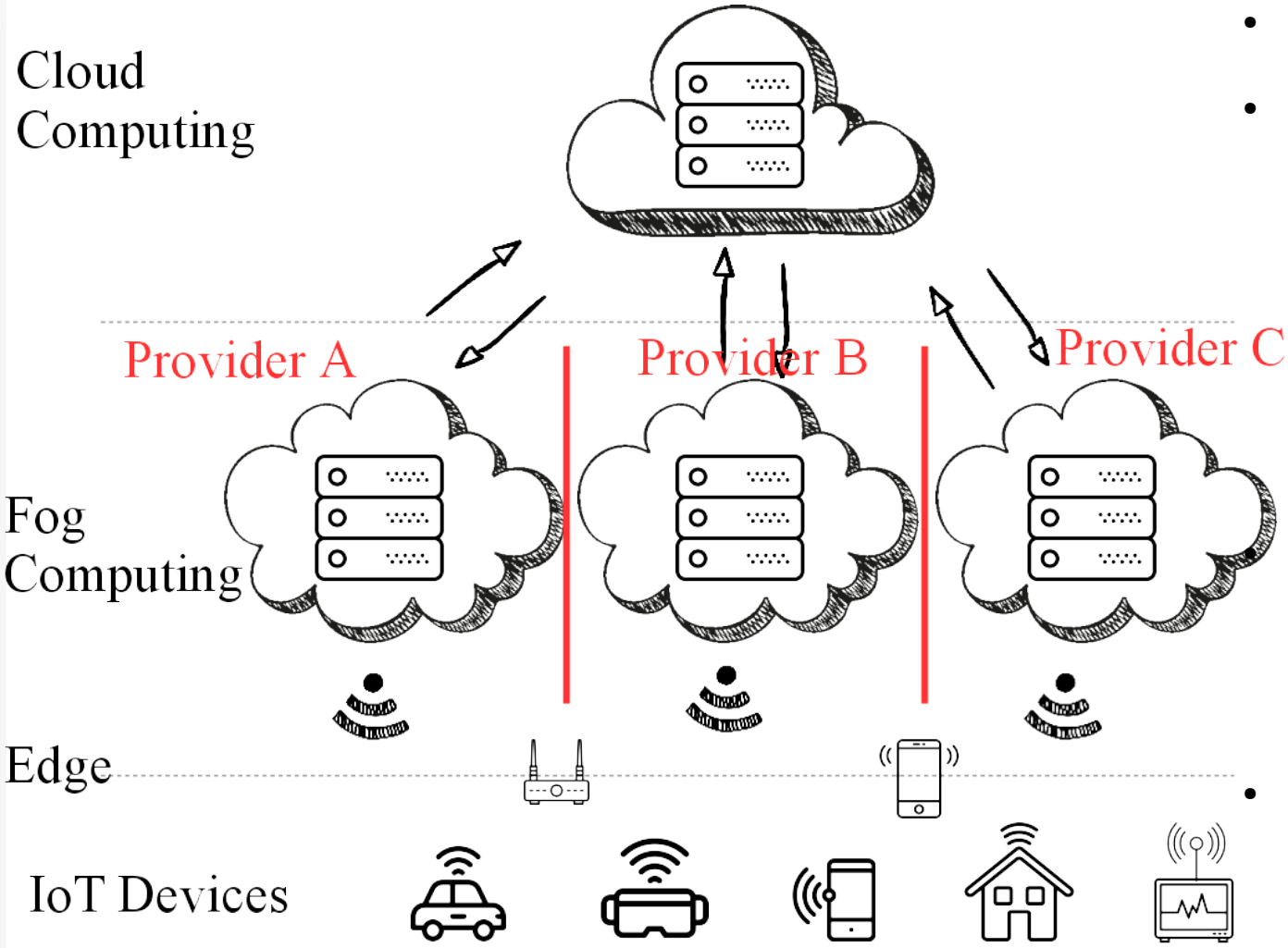
- Store data locally
- Maybe use mobile phone as proxy

- Priorities vs. List of choices (e.g. from traffic control center)

Data Isolation at Different Entities



Data Isolation at Different Entities

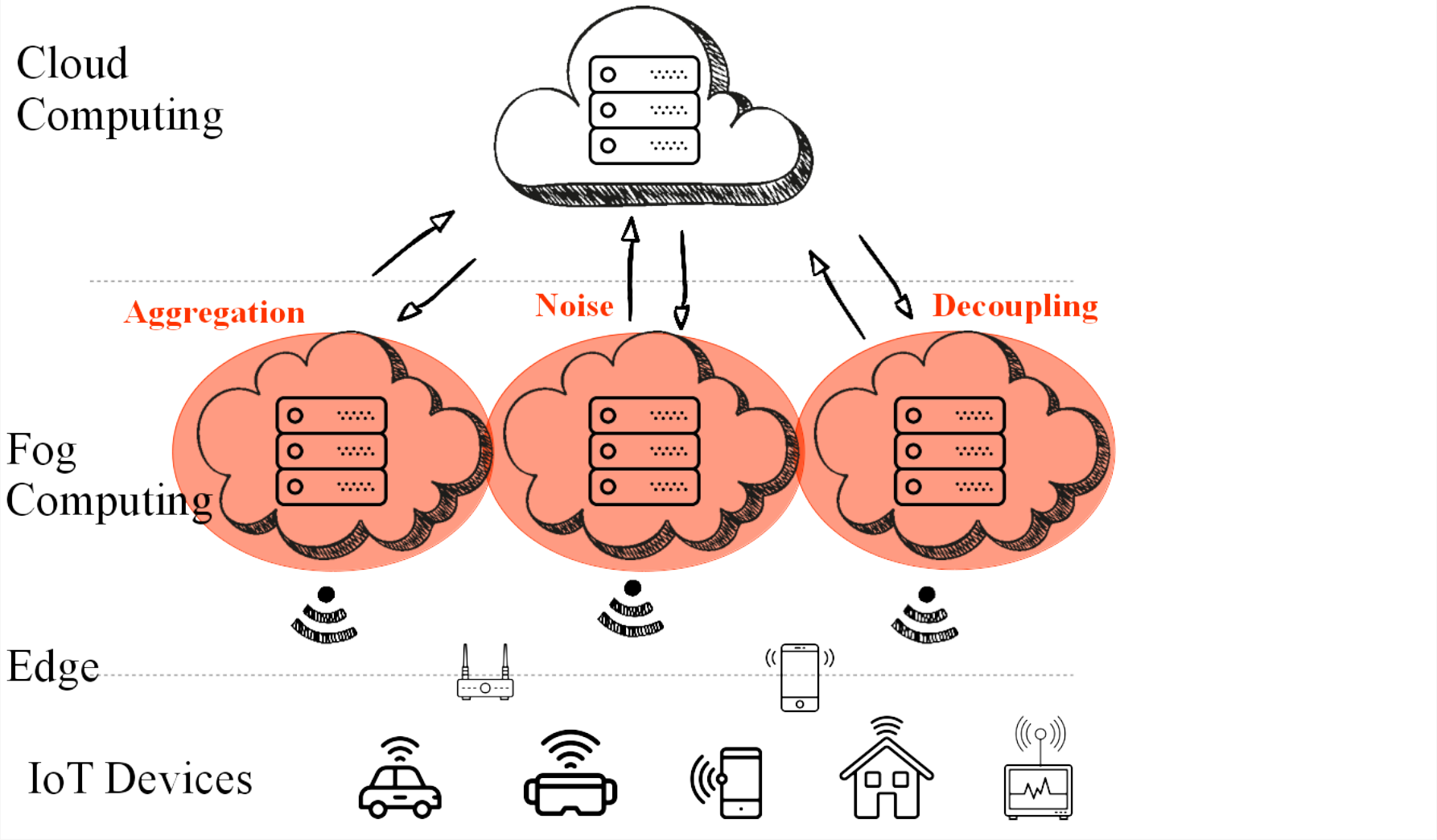


- Distribute data
- Each entity only sees a part

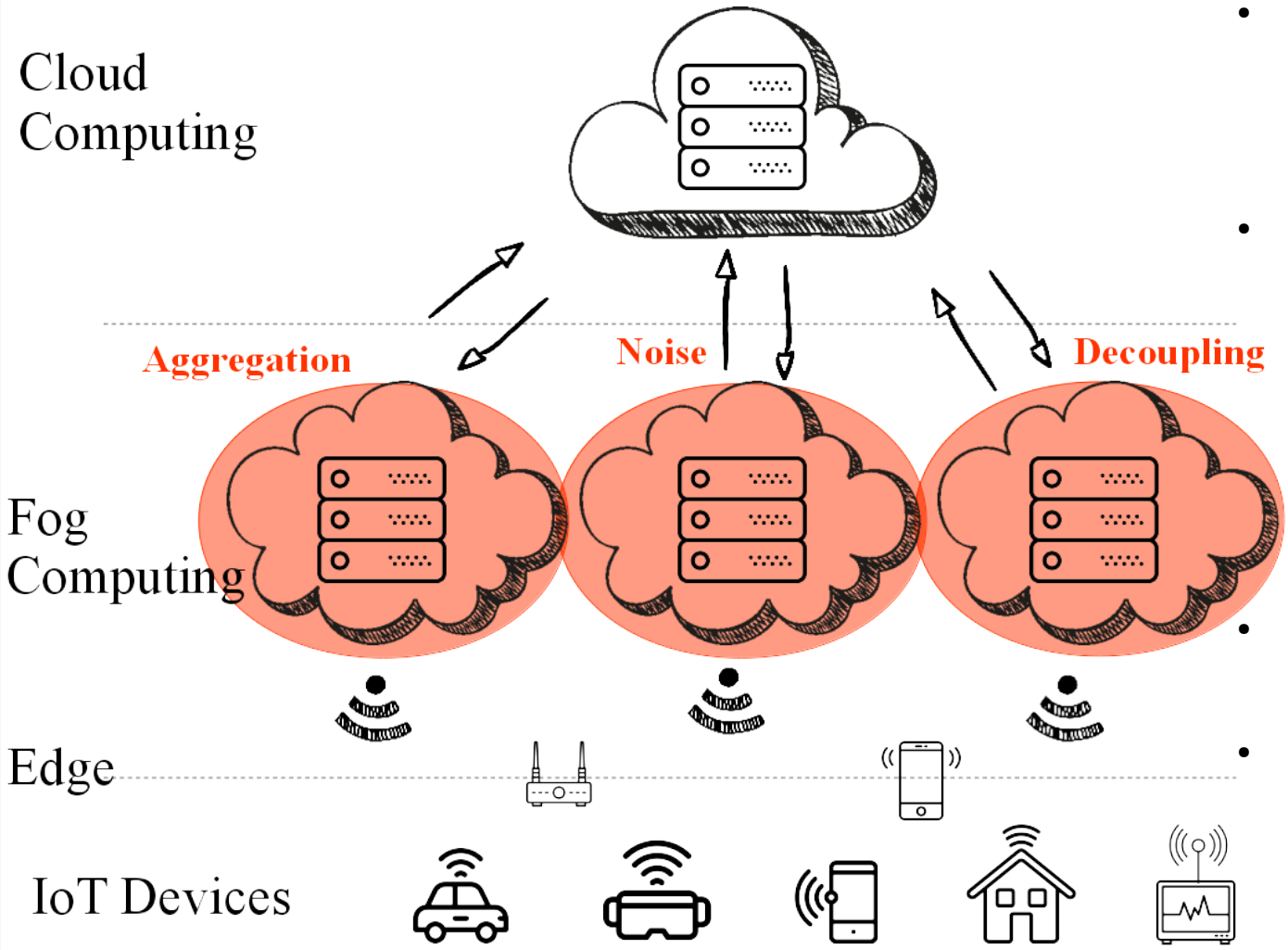
e.g. different habits at different locations

- No profile / sharing

Added Noise Measurement Obfuscation



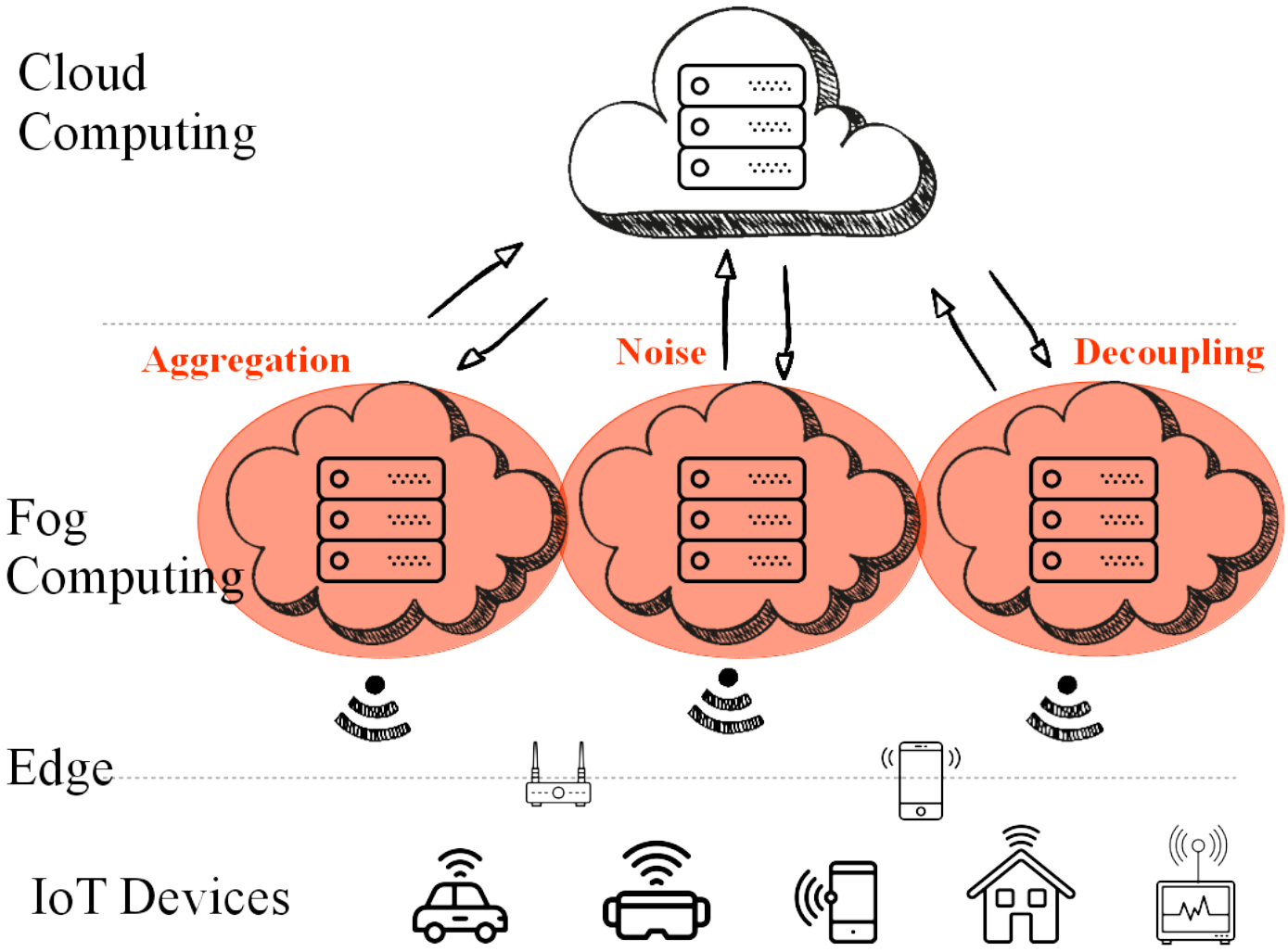
Added Noise Measurement Obfuscation



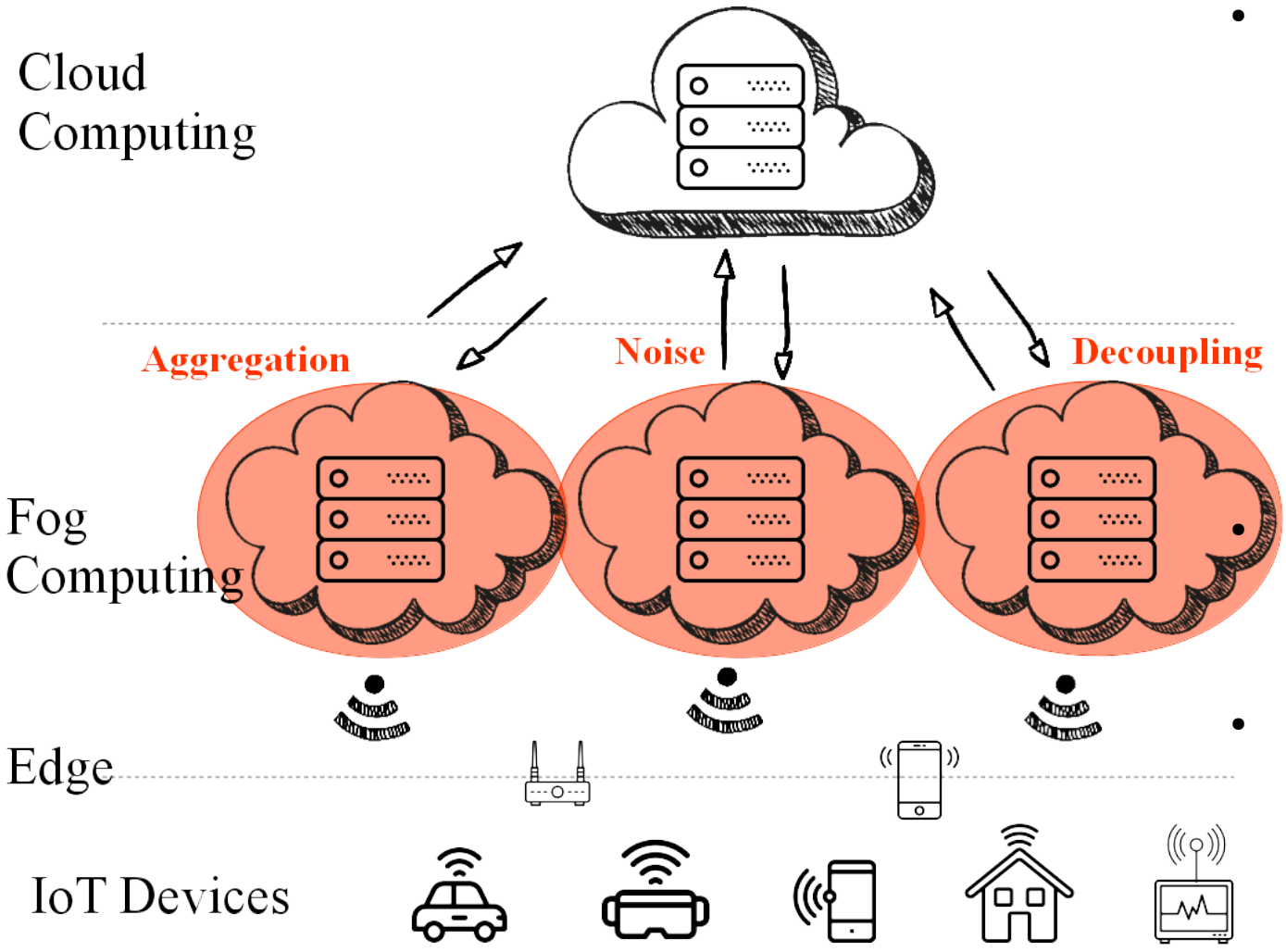
- Continous measurement may leak more data
- If fog node is trusted, fog may add noise

- e.g. give only rough location
- Depends on area a fog node is responsible for

Data Aggregation



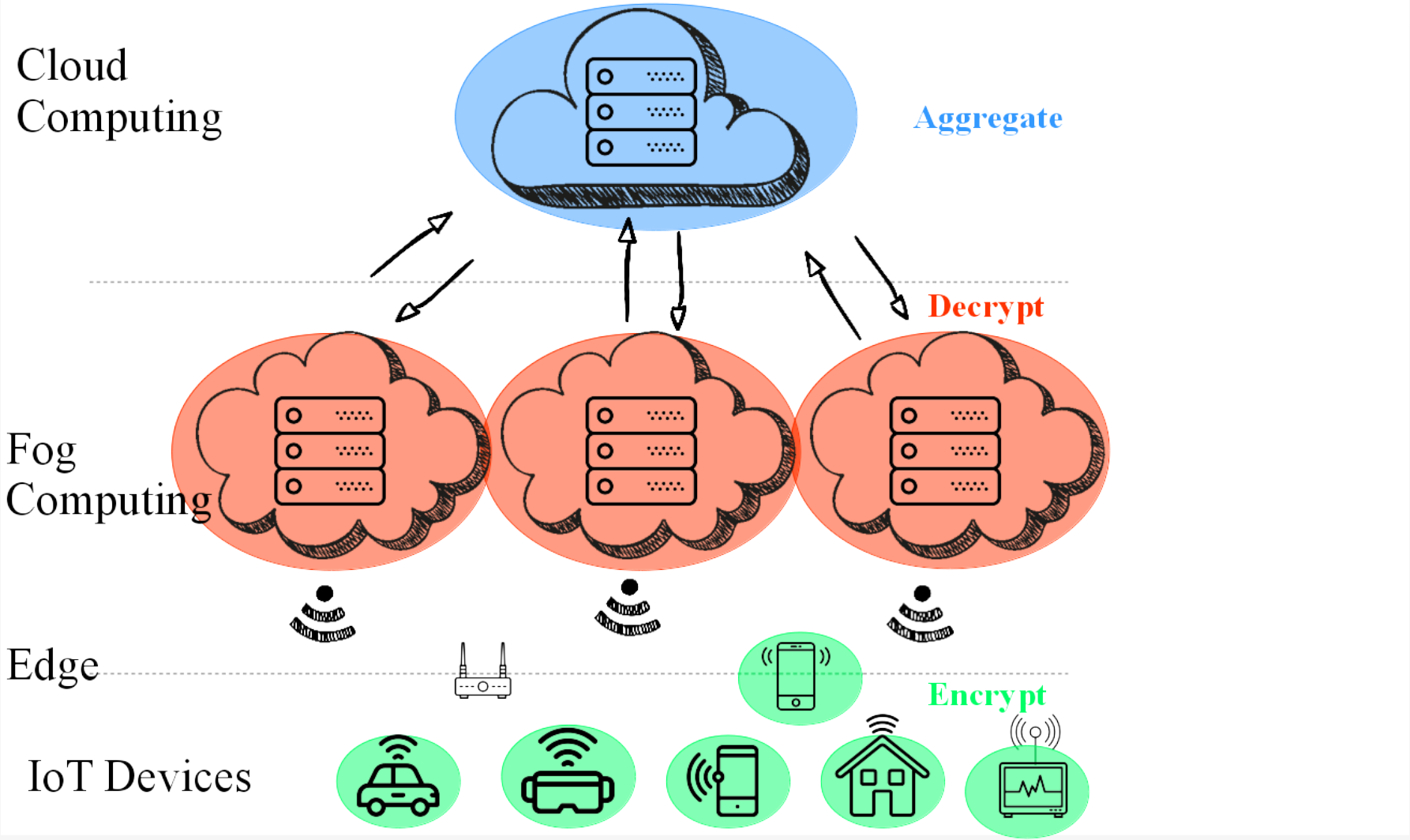
Data Aggregation



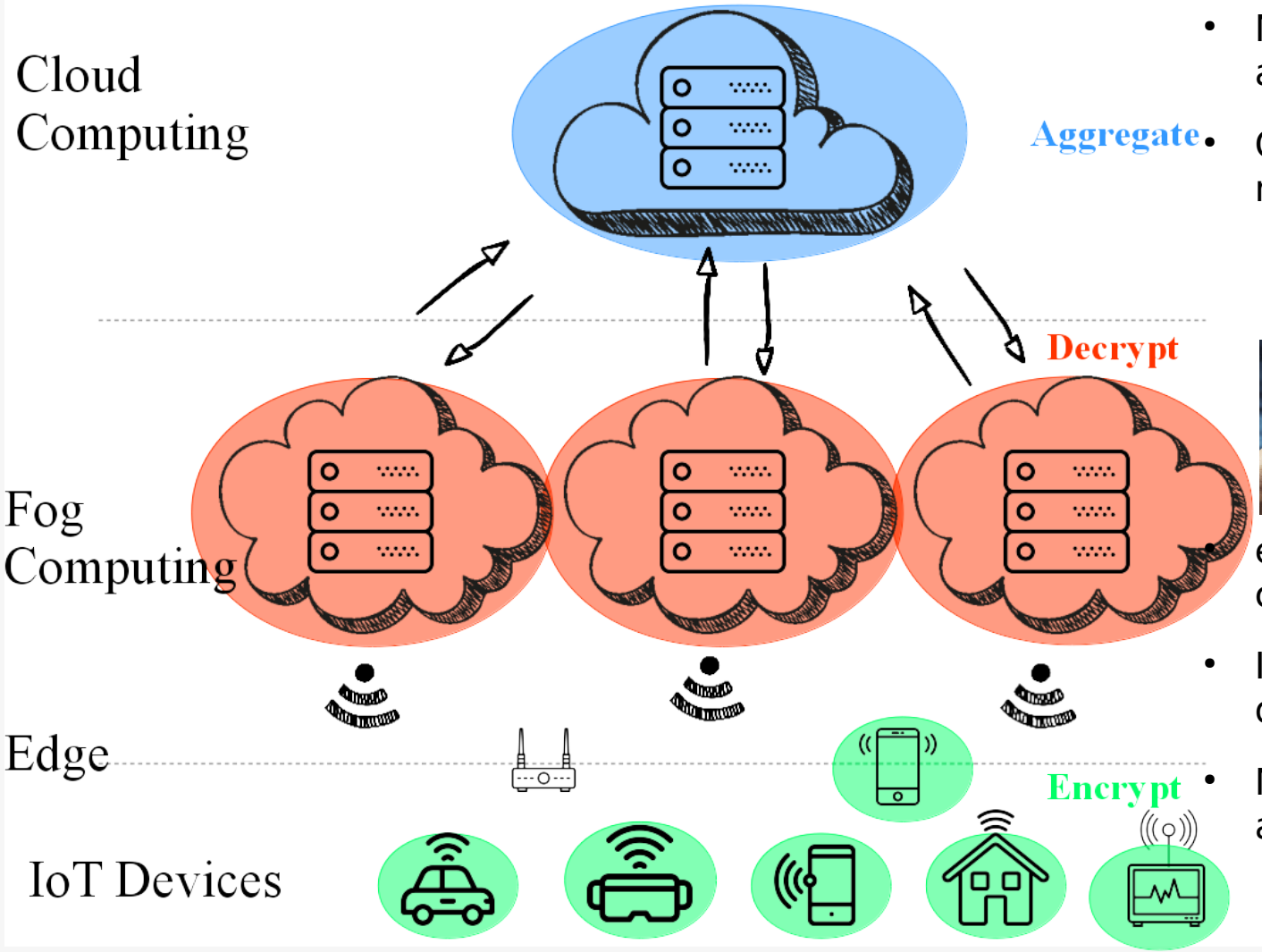
- Instead of adding noise aggregate data

- e.g. usage rate of parking lot
- No profile / sharing

Aggregration Gateway



Aggregration Gateway



- No noise acceptable
- Continous measurement

- e.g. emission of cars
- Impact of air quality
- No information about individuals

Conclusion

- Applying existing patterns in a new scenario is worth it
  - No need to reinvent the wheel

- Several trade-offs necessary
  - Security of cloud / fog / IoT nodes
  - 3rd party / personal control of data
  - User control easier if data is
    - Distributed across fog nodes
    - Stored „centralised“ in the cloud
  - Privacy / performance

Skills

- Applying existing patterns in a new scenario
  - Includes finding / matching them
- Judging criticality of data
- Trade-offs to balance interests / requirements
- Legal skills (GDPR)
- Relation to business models

Chair of Mobile Business & Multilateral Security

Dr. Sebastian Pape
Goethe University Frankfurt
E-Mail: sebastian.pape@m-chair.de
WWW: www.m-chair.de